***BackGround for the problem beginning:***

Together with their constantly growing overall complexity, current

automobiles also offer an increasingly powerful multimedia

environment to the driver and the other occupants.

Having started with simple radio systems and later the

integration of mobile telephones and CD players, today complete

multimedia environments have become available. These are

usually managed by a central on-board computer, which integrates

a variety of audio based systems like radio, telephone and

CD/MP3 players with audiovisual systems like navigation systems,

(HD) DVD/BluRay players and television or head-up displays. In

the automotive domain there is a large amount of information

provided by the multimedia systems to the car occupants, which

also requires much interaction with the system, especially by the

driver (e.g. the interaction with the navigation system).

**Reason for the Weakness of the Automotive Security :**

Inherent weaknesses: In [3], it has been highlighted that

of the weaknesses of vehicles security arise from the

rties of the CAN bus itself such as:

Broadcast Nature

Since the bus has a broadcast nature, then any node

connected to the bus can listen to all data exchanged.

Fragility to Denial of Service (DoS)

Based on the arbitration scheme of CAN, any node can

put the bus in a dominant state preventing other nodes

rom sending any messages.

Absence of authentication

The CAN message itself does not contain any authentica-

ion information about its sender. Thus, it is possible for

any attacker who connects to the bus to send messages

using the identity of any trusted node.

Weaknesses due to deviation from standards: In addition

e weaknesses mentioned above, there are also some

nesses that arise from deviating from security standards

egulations.

Reflashing the ECU should be allowed when the car is

stationary only. However, it was possible to reflash some

ECUs in a moving car.

The key used for reflashing ECUs should be different

rom an ECU to another. However, it was found that

sometimes all the cars have the same key for a certain

ECU.

Standards specify that a CAN gateway can be reflashed

only from the high speed network; and not from the

ow speed network. However, it has been discovered that

a gateway can be also reflashed from the low speed

network.

•

The stored keys in each ECU shall have restricted access

so that they cannot be disclosed easily. However, it was

possible to retrieve some keys from ECUs.

D. Impact of attacks

The highlighted weaknesses in the security of in-vehicle

networks could attract the attention of criminals. Basically,

thieves may be able to locate cars, unlock the doors and steal

them. It could be also possible to extend the attacks to include

several cars in a city simultaneously causing severe accidents.

E. Motivation of the paper

Based on the risks highlighted above, it is important to find

ways to enhance the security of vehicles. The paper focuses

on one of the major security requirements for in-vehicle

networks which is message source authentication. The paperorganized as follows. The next section shows the related work

that has been published. Then, a lightweight authentication

protocol is proposed to be used for CAN networks. After that,

we analyze the protocol and compare it with other protocols.

is